WHAT IS CLAIMED IS:

1. A system for providing secure mobile connectivity that implements Mobile IP Home Agent functionality via distributed components, comprising:

a mobile node belonging to a home network located within a secure network; the mobile node having a network interface configured to communicate with other nodes;

a router configured to forward packets between networks;

a Proxy Home Agent (PHA) connected to the home network and located within the secure network that is configured to provide a portion of the Mobile IP Home Agent functionality;

a Home Agent (HA) located outside of the secure network that is configured to provide another portion of the Mobile IP Home Agent functionality; and

a VPN gateway coupled to the router and the secure network and configured to work in conjunction with the PHA and the HA.

2. The system of Claim 1, wherein the VPN gateway and the HA are located within a single device within a DMZ.

3. The system of Claim 1, further comprising a firewall coupled to the secure network and the VPN gateway; wherein the HA is located within the firewall.

4. The system of Claim 1, wherein the HA is a separate device from the VPN gateway.

5. The system according to claim 1, further comprising:

a DMZ located outside the secure network, wherein the VPN gateway and the HA reside in the DMZ; a first firewall between the secure network and the DMZ; a second firewall between the DMZ and an external network configured to deny communications from the external

network with a source address in the known range; and wherein the mobile node has a permanent address in a known range.

6. The system according to claim 1, further comprising:

a DMZ located outside the secure network, wherein the VPN gateway and the home agent reside in the DMZ; a first firewall between the secure network and the DMZ; wherein the mobile node has a permanent address in a known range and the first firewall is programmed to deny all communications from the DMZ with a source address in the known range; and wherein the VPN gateway has a direct connection to an internal interface of the first firewall such that the first firewall considers the VPN gateway transmitted data as internal to the secure network.

7. The system of Claim 1, further comprising a DMZ comprising a first router coupled to a second router that is coupled to a firewall, the VPN gateway coupled to the first router and the firewall; the HA coupled to the router.

8. The system of Claim 7, wherein packets from the MN destined toward nodes inside the secure network first go the HA and then to the VPN gateway that is configured to forward the packets through the firewall to the secure network.

9. The system of Claim 8, wherein packets from the second router to the firewall having a source address in a known range are dropped by the firewall.

10. The system according to claim 1, wherein the router is directly connected to a firewall and the VPN gateway and the HA connect to a different interface of the router and the firewall.

11. The system of Claim 10, wherein the firewall is configured such that it considers the interface with which it connects to the VPN gateway as an internal interface and packets with

a source address that are outside of a known address range received on the internal interface are dropped, and packets with a source address that are within the known address range that are received by the firewall on an external interface are dropped.

12. The system of Claim 11, wherein VPN encapsulated packets are forwarded to the VPN gateway and when a Security Association (SA) exists, the packet is decrypted and forwarded to the firewall on the internal interface and when a SA does not exist the packet is dropped.

13. The system of Claim 12, wherein Mobile IP packets and VPN encapsulated packets first reach the Home Agent which are forwarded to the VPN gateway and then to the secure network through the firewall's internal interface.

14. The system of Claim 1, further comprising a firewall coupled to the secure network and the VPN gateway; wherein the router includes an access control list used to drop packets that have a source address that belong to a known address range.

15. A method for secure communication between a mobile node associated with a home network in a secure network and a correspondent node; comprising:

establishing a Proxy Home Agent (PHA) located within the secure network to monitor data directed to the mobile node;

establishing a Home Agent configured to create a security association with the mobile node;

collecting data directed to the mobile node;

packaging the collected data in a VPN secure tunnel to an internal address of the mobile node to create VPN packaged data; and

tunneling the VPN packaged data to a current address of the mobile node.

16. The method of claim 15, wherein the VPN secure tunnel follows the IP security protocol.

17. The method of claim 15, wherein the tunneling of the VPN packaged data to the external mobile node occurs according to the IP mobility protocol.

18. The method of Claim 15, further comprising: packaging the collected data in an IP-in-IP tunnel and sending it to a VPN device for VPN encryption and tunneling the VPN packaged data to the current address of the Mobile node.

19. A system for secure mobile connectivity that implements Mobile IP Home Agent functionality via distributed components; comprising:

means for establishing a Proxy Home Agent (PHA) located within the secure network to monitor data directed to the mobile node;

means for establishing a Home Agent configured to create a security association with the mobile node;

means for collecting data directed to the mobile node;

means for packaging the collected data in a VPN secure tunnel to an internal address of the mobile node to create VPN packaged data;

means for tunneling the VPN packaged data to a current address of the mobile node;

means for the Home Agent to communicate to the PHA that the mobile node has moved outside its home network; and

means for the Home Agent to communicate to the PHA that the mobile node has come back to its home network; and

means for enabling the PHA to create and remove a proxy ARP entry for a permanent address associated with the mobile node.